A New Digital Signature Algorithm for Ensuring the Data Integrity in Cloud using Elliptic Curves

Balasubramanian Prabhu Kavin[1] and Sannasi Ganapathy[2]
[1]Sri Ramachandra Institute of Higher Education and Research, India
[2]Centre for Cyber-Physical Systems and School of Computer Science and Engineering, Vellore Institute of Technology, India

Abstract: *In this paper, we propose an Enhanced Digital Signature Algorithm (EDSA) for verifying the data integrity while storing the data in cloud database. The proposed EDSA is developed by using the Elliptic Curves that are generated by introducing an improved equation. Moreover, the proposed EDSA generates two elliptic curves by applying the upgraded equation in this work. These elliptic curve points were used as a public key which is used to perform the signing and verification processes. Moreover, a new base formula is also introduced for performing digital signature operations such as signing, verification and comparison. From the base formula, we have derived two new formulas for performing the signing process and verification process in EDSA. Finally, the proposed EDSA compares the resultant values of the signing and verification processes and it checks the document originality. The experimental results proved that the efficiency of the proposed EDSA in terms of key generation time, signing time and verification time by conducting various experiments.*

Keywords: *Cloud, digital signature, enhanced digital signature, elliptic curve, signing process, verification process and comparison.*

Received August 13, 2019; accepted June 17, 2020
https://doi.org/10.34028/iajit/18/2/6

1. Introduction

The enhancement and the globalization of computer networking technology using internet services are known as cloud today. The cloud computing technology is created to satisfy the properties such as high quality and consistent service, resources with rapid elasticity, service provided based on the requirement and extensive access of the network [25]. The data outsourcing process is difficult and not possible in traditional computing technology. Moreover, the data outsourcing process is the main key process in cloud computing. The property of outsourcing that provides the Information Technology (IT) vendors and the individual users to store large volume of data in the cloud with less expense [26, 32].

Cloud storage is considered as one of the important techniques due to its higher efficiency and lesser utilization cost. In the cloud data storage, the data centers are shifted to pools of large-scale computing services by using the service called as "software as a service". The user's data that are residing on the remote data centers can be accessed easily by using the high-quality network connection [25]. Jaidi *et al*. [10] has done a higher-level integrity analysis over the access control policies. Cloud storage facilitates the data accessibility to the cloud users from any different geographical locations with huge storage space which is not possible in the traditional storage technologies. Moreover, the cloud users can access the data by using any type of network devices that are connected to the internet. Even though, the data security is a challenging issue due to the arrival of huge number of cloud users. In this scenario, the introduction of data security mechanism is necessary for overcoming the data security issues. Here, the Cloud Service Provider (CSP) is the provider of services for the cloud users depending upon their requirements.

The CSP provides their own security service to the storage space that facilitates for the authorized cloud users. Moreover, the cloud user stores their own data securely in cloud storage space but the storage space is not trustworthy because the CSP is a third-party vendor. In this case, the cloud user's data is in risk at cloud database. In particular, the genuine user's data can leak by the attacker using virtual machine side channel attack [28]. In addition, the data lose problem occurs everywhere in any type of the cloud framework even though it is protected with high security features. Occasionally, the CSP eliminates the data that are not used frequently by the user. Moreover, the CSP pretends that the cloud user's data are available even after losing them [18, 23]. Finally, the cloud users should be prepared to face such type of the data losses. This kind of the security drawbacks will stop the individual from outsourcing the data in the cloud. It also slowdowns the wide spreading cloud computing technology.

The verification is an important task which is used to authenticate the user's data and ensure the data

integrity in cloud environment. This verification process reduces the vulnerabilities of data theft. In public verification process, the liberated third-party auditor is the classic method which is used to verify the data that are stored in the cloud storage [12]. This type of approach is adopted and used in various security models [15, 28]. The third-party auditor does all work that is related to auditing by communicating with the cloud users and the cloud service providers and collect the required information for verifying the data integrity. In addition, it is not necessary to reveal the auditing process done by the Third-Party Auditor (TPA) to the cloud user. Rather, the TPA sends the detailed report about the auditing process to the cloud user with the integrity verification history of the user's data stored in the cloud. This process facilitates to receive the verified data by the cloud users without any extra effort by employing the TPA. The basic features of the efficient TPA such as they should not copy any data and should not introduce any new risk factors to the users [18].

A digital signature is the process of signing the electronic document which will be sent to the receiver to make him believe that the document is genuine with the sender's signature [32]. There are two important reasons for adopting digital signature instead of analog signature. First, the duplication is possible in analog signature even though it is complicated where the digital signature is unique. Second, the analog signature of an individual user or document is same in all the documents and records whereas in digital signature it is completely different. The signature differs for every document based on the specific document information [26]. The fundamentals of digital signature algorithms are discrete logarithms. The digital signature mechanism is responsible for performing four kinds of services like data origin authentication, Peer entity authentication, nonrepudiation and data integrity.

Elliptic curve cryptography is the algorithm in which the elliptic curve is used in the finite field (i.e.,) fixed number of elements. The cryptographic applications are classified in to two types of elliptic curves, one is binary curves G.F (2n) and the other is prime curves Zp. Many researches have been emerged in public key cryptography by utilizing elliptic curves, one among them is a Digital Signature Algorithm with elliptic curves Digital Signature has received the Digital Signature Standard (ECDSA). Moreover, the Elliptic curve (FIPS 186-2) in the year of 2000. ECDSA provides double security level while comparing RSA digital signature. In the 80 bits security range the attacker needs to generate 280 different signatures to find the private key. 1024 bits are the least bit sized public key of the Digital Signature Algorithm (DSA) while the least public key size of the ECDSA is 160 bits. Though, the DSA and ECDSA have bigger differences in their key size the signature length of both the scheme remains same [23].

The novelties of this newly proposed digital signature algorithm are:

1. Applied Elliptic Curve Cryptography Square (ECC^2) for generating public keys.
2. Introduced a new formula for performing, signing process.
3. Introduced a new formula for performing verification process.
4. Applied "modulo" function for signature compression.
5. Introduced new signature reference table for creating an efficient signature.

Remainder of this research article is formulated as below: section 2 summarizes the advantages and disadvantages of the existing works that are available in this direction in the past along with the highlights of their works. Sketch the overall proposed system architecture and explain the functionalities in section 3. The necessary background and explanations of the proposed digital signature algorithm along with the suitable example is provided in section 4. Section 5 demonstrates the experimental setup and obtained results with justification for the enhancement. The proposed work is concluded with possible future works in section 6.

2. Literature Review

The enormous volume of digital signature schemes and cloud data security mechanisms have been proposed in the past two decades for securing the data in networks and cloud environment [9, 16, 17, 22, 24, 32, 35]. Among them, Chen *et al*. [5] proposed a new signature pattern by enhancing the existing chameleon hashing scheme. In their work, the key is not exposed because that applies triple door mechanism for providing the solution for handling the sensitive issues. Moreover, they introduced a new signature pattern to attain the properties that are required to improve the data security. Kim and Oh [14] developed a novel signature scheme for storing the signatures and keys securely in communication. In their scheme, the length of the aggregate signatures, secret keys, and public keys are fixed. Moreover, they have collected the third party's signature in their scheme for performing verification process. Xue *et al*. [31] developed a management agency to provide the special right to the root by applying a digital signature. Moreover, they have provided an authentication scheme for the application with guaranteed root privilege by adopting the digital signature.

Zhang and Wang [35] proposed an enhanced digital signature scheme by relying on the classical digital signature method to conquer the forgery attack. Their scheme does not have a one-way hash function. In

addition, they also have been done the security analysis for their system. Gao *et al*. [6] designed an enhanced chameleon hashing method which depends on Schnorr signature to prevent the key leakage, message hiding, security semantics and resisting the collision.

Bjelland *et al*. [2] presented three-way operations for performing the exact matching by applying Approximate Hash based Matching where clustering, searching and streaming are the three operations. This system has provided a solution for the data similarity problem during the process of digital investigation process. Zhang [34] developed a new combined approach by integrating digital signature and fault tolerance in Rivest, Shamir, Adleman (RSA) to identify and rectify the errors occurring in both computing and transmission processes. Their approach is designed for the other public key cryptography methods. Lou and Liu [20] developed a novel digital signature method with the property of compression tolerating and fault resisting which is based on the public key for providing authenticity through verification and data integrity.

Bellare and Neven [1] developed a new signature scheme that works based on factoring to avoid the forgery in the standard model. In their scheme, the signature is shortened and eliminates the node certificates by introducing modifications according to the hash factoring, gap diffie hellman and RSA. Chang and Chang [4] proposed a new methodology for signing the digital signature in which not used the message redundancy schemes and one-way hash function. Moreover, the system is completely against the forgery attacks. Even though, their signature does not follow the traditional security techniques, protects the scheme and maintains the properties of the traditional methods.

Li *et al*. [18] presented a new Cryptography-based Data Publishing System (CDPS) for maintaining the integrity of the data and for attaining invisibility property without any data loss. This system is proven to be secured while comparing with the traditional security scheme. The CDPS was defined only for some specific data processing needs and it considered as the drawback of their system.

Kaaniche and Laurent [12] conducted a survey on the data privacy and the data security problems that are encountered by the users in the cloud computing environment. In addition, they compared the existing cryptographic techniques and also discussed the recent cloud data security schemes. Jiang and Guo [11] developed an efficient data sharing method for sharing the data effectively in cloud environments. In their method, the encrypted data sent to the cloud for secured storage. Moreover, their method incorporates the proxy broadcast and re-encryption technique for performing dynamic sharing in which the user can be added and removed dynamically from the group. They method achieved improved sharing performance, proven security and accuracy. Sohal and Sharma [27] developed a novel cryptographic method for encrypting the client's data that are stored in cloud database. Here, they compared their work with traditional symmetric key algorithms and concluded that their method is better in terms of encryption time, throughput and ciphertext length. Yu *et al*. [33] proposed a new encryption scheme called two round searchable encryption scheme for eliminating the data leakage from cloud environment.

Liu *et al*. [19] suggested a new multiple-owner sharing scheme for sharing the data securely in the cloud environment that is applicable for performing dynamic groups. Tysowski and Hasan [29] presented a new enhanced attribute-based encryption to secure the cloud user data. The computational process is completely given to the CSP and reduces the computational cost. Zhou *et al*. [36] designed a hybrid cloud storage architecture that integrated with role-based architecture to store the organizational data in a public cloud. The CSP performs the processes by using the public key when the user holds a single private key. Huang *et al*. [7] developed a new key management and access control method for storing the data securely in a cloud environment. Their method evolved from the proxy re-encryption and the attribute-oriented encryption process. Moreover, their method was proven as an efficient practically in terms of security.

Mitchell [21] introduced a secured technology for the encryption process which is named as two key triple DES. The bit length of this newly proposed encryption technique is 80 bits. Wang *et al*. [30] developed an enhanced version of the AES encryption technique that is based on the nanowire for the purpose of increasing the energy efficiency and the throughput level. Tysowski and Hasan [29] recommended an integrated mechanism for managing the keys in the cloud environment. This system is to protect and to increase the key size of the mobile application when it is required. Re-encryption and hybrid attributes are the two techniques combined together in this work.

Huang and Wang [8] developed an efficient and very larger key size design for RSA to improve the complexity of the encrypted data prediction. Kavin and Ganapathy [13] proposed a new chinese remainder theorem based data storage mechanism for performing secured data storage in cloud environment. Moreover, they have developed a new group key management algorithm for providing secure access to the cloud users in a group. Their mechanism achieved higher security level by increasing the prediction complexity.

This section described the various works in the field of cryptography, encryption, decryption, digital signature, key generation, signature verification, secured storage in cloud and privacy preserving mechanisms in the past. All these mechanisms have been achieved better performance than their existing works that are available in the literature in the same directions. Even though, these all systems and

mechanisms are not satisfying this fast world requirements in terms of data security and data authenticity while accessing the cloud data and also restricting the unauthorized cloud user's accesses in cloud.

3. System Architecture

The overall system architecture of the proposed model is shown in Figure 1. It consists of eight components such as cloud user, encryption process, cloud database, decryption process, authorized cloud user, signing module, third party auditor and verification module.

- Cloud user: the cloud user sends the data/ document into the encryption process component of this architecture for encrypting the data/document. The encrypted data/document is stored in the cloud database for further processes.
- Encryption process: the encryption process component is responsible for encrypting the cloud user data/document and it stores the data securely in cloud database.
- Cloud database: the role of cloud database is to maintain the encrypted data/document that is sent by the various cloud users. It allows the authorized cloud users to access the stored data/document through the cloud service provider.
- Signing module: the signing module creates the digital signature of the original data/document which is sent by the cloud user. First, the SHA 512 hash function which is used for extracting the hash message of the original document. Here, the public keys were generated by using the elliptic curve square. The hash message will be processed along with the generated public keys. By applying the newly proposed signing formulas, the digital signature is created. This digital signature will be sent along with the encrypted document to the cloud database for further process.
- Third party auditor: the Third-Party Auditor (TPA) is responsible for managing and maintaining the signing and verification processes. The cloud user need not to worry about the document is stored/copied by the third-party auditor. The TPA only responsible to verify the document without the knowledge of the cloud user, another user cannot access any document.
- Authorized user: the authorized user gets authorization for accessing the specific document which is stored by the cloud user in an encrypted format with a signature. The encrypted document will be accessed and it will be decrypted using the decryption process. Now, the authorized user has the original document along with a digital signature that is created by the cloud user. The authorized user will verify the originality of the document with the help of TPA.
- Decryption process: the decryption process component is used to decrypt the cloud user data/document that is stored in the cloud database to get the original document.
- Verification module: the verification module verifies the digital signature of the original data/document which is sent by the authorized user. First, the message digest will be created by applying the generated key values in the newly proposed verification formulae.

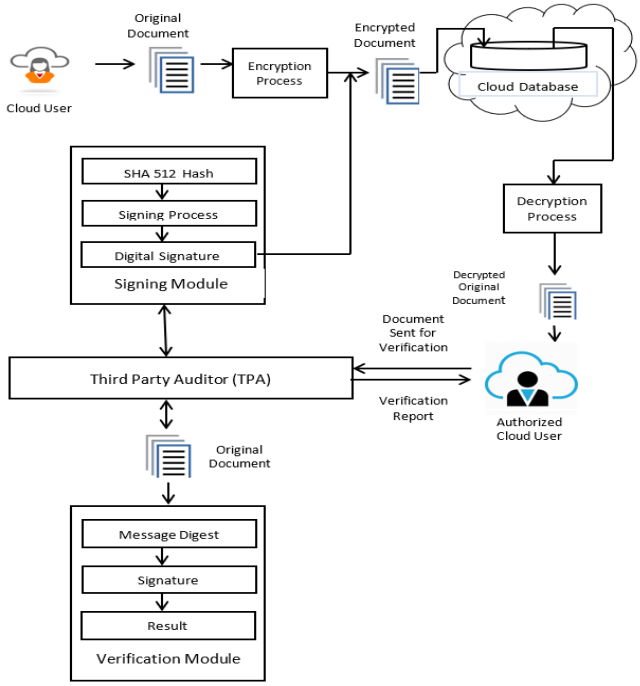

Figure 1. System architecture.

A new signature will be created by applying the verification formula. The signature, which is available along with the original document will be compared with this new digital signature. If both the signatures are same then the integrity of the document is perfect otherwise the accessed document is modified document or fake document.

4. Proposed Work

This work proposed an EDSA for secured data storage in the cloud and access from cloud database. This proposed EDSA is developed based on Elliptic Curve Square which is generated by using an upgraded equation. The proposed EDSA generates two elliptic curves by applying the upgraded equation in this work. These elliptic curve points were used as a public key which is used for performing the signing and verification processes. Moreover, a new base formula is also introduced for performing digital signature operations such as signing, verification and comparison. From the base formula, we have derived a new formula for performing the signing process in EDSA and also generate a new formula for performing verification process. Finally, the EDSA compares the

resultant values of signing and verification processes. The document originality is checked by using this comparative result as same otherwise the document is not same/genuine. This proposed work is explained under six subsections such as rational function for digital signature, key generation process, hashing, signing process, verification process and comparison process. The working flow of the proposed enhanced digital signature algorithm is shown in Figure 2.

First, the original data is signed by using the signing phase of the enhanced digital signature algorithm. In signing phase, the hashed message of the original data is created using Secure Hashing Algorithm (SHA) 512 hash function. The digital signature is generated using the public keys that are created by the points of the elliptic curve square. Now, the 8 bits of 248 bits are processed by applying the compression formula to get 64 bits signature. This signature is stored along with the encrypted data in cloud database. Later, the authorized user will access the original data that is stored in the cloud database to check the integrity of the data using the verification process.

The verification process can be done by comparing the digital signature in the original data and the new signature created by the instant document. If both the signatures are same then the accessed data is original otherwise it is fake or not genuine. Now, the detailed description of the proposed EDSA is explained in the further subsections.

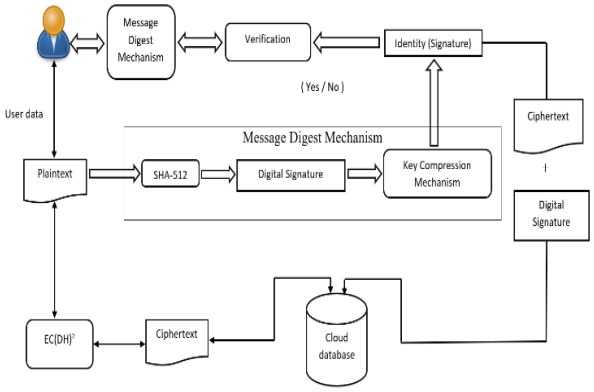

Figure 2. Working flow of EDSA.

4.1. Rational Function for Digital Signature

A rational function (or univariate rational function) (Blahut [3]) is an expression of the form f(x)/g(x) where f(x) and g(x) are polynomials with coefficients in F. Division of a rational function by f(x)/g(x) is defined as multiplication by g(x)/f(x) provided f(x) is nonzero. A monic rational function is a rational function in which the leading coefficients of f(x) and g(x) are both equal to one. We will also make use of F[x, y] and F(x, y), the rings of bivariate polynomials and bivariate rational functions, respectively.

In this work, we have introduced the developed version of a new advanced formula based on the algebraic formula with the consideration of parameters that are available in digital signature standards as a base formula for performing digital signature processes. The new base formula is shown in Equation (1).

$$\left[\frac{h^2-(H(M)*h}{h^2-(k*m)}\right] mod\ p = 1 - \left[\frac{(H(M)*h)-(k*m)}{h^2-(k*m)}\right] mod\ p \quad (1)$$

Where p represents the random prime number and also using the p value in the mod function to bounded the size of the function, H(M) indicates the Hashed Message, h represents the hashing value, k and m are indicating the public keys that are generated from the Elliptic Curves.

This new base formula consists of Left Hand Side (LHS) and Right Hand Side (RHS) where LHS, part of the formula is used to perform the document signing process and the RHS part of the formula is used for performing the verification process in digital signature which taken care by the third party auditor.

4.2. Key Generation Process

This subsection consists of sections such as elliptic curve and Elliptic Curve square (EC^2). Here, the elliptic curve is providing a single curve by applying a standard equation and the EC^2 is providing two curves by applying a newly upgraded equation which is upgraded from the standard elliptic curve equation. The elliptic curves are used to perform key generation in the digital signature process.

4.2.1. Elliptic Curve

The term "Elliptic" is not meant that the equations are ellipses. Here, the common structure of the elliptic curve formula is given in Equation (2).

$$y^2 = x^3 + ax + b \quad (2)$$

Where 'a' and 'b' indicate the real numbers. Let consider 'a' holds the value of 2 and 'b' holds the value of 1. The curve which is generated by the standard Elliptic Curve Equation is shown in Figure 3.

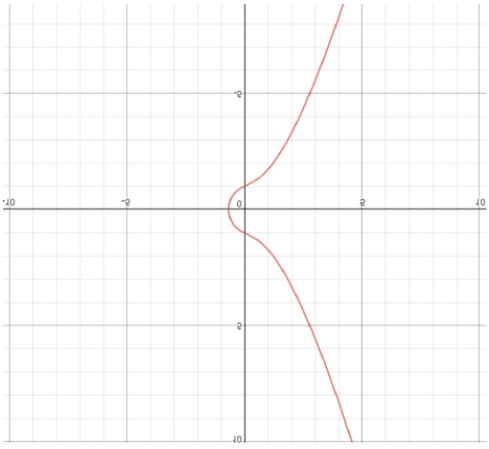

Figure 3. Elliptic curve.

This elliptic curve is useful for performing the key generation process by using any point randomly which is available on the elliptic curve.

4.2.2. Elliptic Curve Square (EC^2)

The square EC^2 is generated by using a new upgraded formula that performs the square operation over the standard elliptic curve formula which is given Equation (2). The elliptic curve square equation is generated as follows:

$$y^2 = x^3 + ax + b$$
$$(y^2)^2 = (x^3 + ax + b)^2$$
$$y^4 = x^6 + 2(ax + b)x^3 + a(ax + 2b)x + b^2$$

The upgraded formula is generated from the standard formula and shown in the Equation (3):

$$y^4 = x^6 + 2(ax + b)x^3 + a(ax + 2b)x + b^2 \quad (3)$$

Where '*a*' and '*b*' indicate the real numbers. Let consider 'a' holds the value of 2 and 'b' holds the value of 1. The curves that are generated by the upgraded EC^2 Equation are shown in Figure 4.

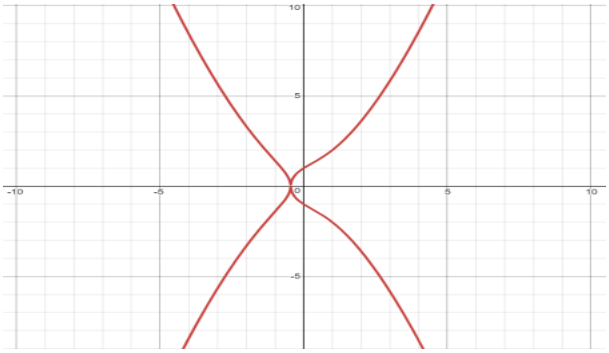

Figure 4. Elliptic curve square.

These elliptic curves are useful for performing the key generation process by using random points that are available in these elliptic curves.

4.3. Hashing

Hashing is a technique which is useful for transforming the characters of an input string into a shorter and fixed length value/key which indicates that the genuineness of the string. Moreover, it is used for performing the indexing process for retrieving the text more efficiently. In addition, hashed key value (h) is used to find the text faster than the original value. In this work, the hashing technique is used to transform with the hashed key value along with message digests (H(m)) are sent to the recipient cloud user for verification purpose by the third party auditor.

The Secure Hash Algorithm (SHA) is a hashing algorithm [4] which is used to generate the fixed length of the message digest for the given input document. The four types of SHA algorithms such as SHA-224, SHA-256, SHA-384 and SHA-512 are available in the family of SHA-2. Generally, all SHA algorithms are the same based on the nature of working procedure. Moreover, the SHA algorithms are differed or varied in bit size of their output.

4.4. Signing Process

The signing process in DSA is the process of hiding the message digest which is in the form of value. In this section, we described in detail about the signing process of the digital signature. Hence, we introduced new formulae which are derived from the LHS of base formula for performing the signing process. The new formulae are given in Equations (4), (5), and (6).

$$S = (h^2 - H(M) * h) mod\ p \quad (4)$$

$$T = (h^2 - k * m) mod\ p \quad (5)$$

$$R = \left(\frac{S}{T}\right) mod\ p \quad (6)$$

Where '*h*' is the hash value, *H*(*M*) represents the hash message which is derived from SHA-512, '*p*' indicates the random prime number, '*k*' and '*m*' are representing the public keys that are generated by using elliptic curves, *R* indicates the resultant value of the signing process, *S* and *T* are used as temporary variables for holding the LHS parts of the base formula.

4.5. Verification Process

This section explains the verification process in the proposed digital signature algorithm. Generally, the verification process is the process of verifying the document/content by using the verification formulae that are shown in Equations (7) and (8).

$$U = (H(M) * h - k * m)\ mod\ p \quad (7)$$

$$V = \left(1 - \left(\frac{U}{T}\right)\right) mod\ p \quad (8)$$

Where '*h*' is the hash value, *H*(*M*) represents the hash message which is derived from SHA-512, '*p*' indicates the random prime number, '*k*' and 'm' are representing the public keys that are generated by using elliptic curves, *V* indicates the resultant value of the verification process, *U* and *T* are the temporary variables for holding the RHS part of the base formula.

4.6. Compression Process

The compression process is performed for reducing the bit size of the signature and it will be used to reduce the space utilization and also reduces the comparison time. The compression process is performed by applying the following formula which is given in Equation (9).

$$C\ mod\ p = D \quad (9)$$

Where *C* indicates the 8 bits of 512 bits message digest, '*p*' is the random prime number and *D* is the compressed 2 bits of the message digest value.

4.7. Comparison Process

This section discussed about the comparison between

the resultant value of signing and verification processes. Here, we fetch the resultant values of signing and verification processes in this work that are stored in the third part auditor.

$$U = V \text{ (U and V should be same)} \quad (10)$$

Based on the comparison result, the third-party auditor will conclude that the retrieved document whether it is a genuine or modified document. In this scenario, the values of U and V must be same to be a genuine document. If it fails to be same, then the retrieved document is a modified or fake.

4.8. Enhanced Digital Signature Algorithm

This paper proposed an EDSA using Elliptic Curves. Here, the EDSA applies the elliptic curve two times for generating the key points that are used as a public key to generate the signature. The steps of the proposed EDSA are as below:

Algorithm 1: Enhanced Digital Signature

Input: Document

Output: Digital Signature

- *Phase* 1: Hashed Message
  - *Step* 1: Read the original document which is to be stored in the cloud database.
  - *Step* 2: Apply SHA-512 hashing function to produce H(M) of 128 bits.
  - *Step* 3: A unique Caesar cipher table is introduced in Figure 5, where row R1 holds the message digest components and R2 holds the key for the corresponding components.

Caesar Cipher table with prime numbers as the key values:

R1	0	1	2	3	4	5	6	7	8
R2	02	03	05	07	11	13	17	19	23

R1	9	A	B	C	D	E	F	G	H
R2	29	31	37	41	43	47	53	59	61

R1	I	J	K	L	M	N	O	P	Q
R2	67	71	73	79	83	89	97	101	103

R1	R	S	T	U	V	W	X	Y	Z
R2	107	109	113	127	131	137	139	149	151

Figure 5. Caesar cipher table.

  - *Step* 4: Compare the message digest with the Caesar cipher table and 256 bits numerical message digest is also extracted.
  - *Step* 5: Each two bits of 256 bits numerical message digest is taken separately as H(M) value and processed along with other keys for generating the signature.
- *Phase* 2: Key Generation
  - *Step* 6: Let consider "p" as a random prime number and "h" as a hashing key which is a random number.
  - *Step* 7: Let consider any two random numbers for the variables "a" and "b" that are applied to ECC[2] equation $y^4=x^6+2(ax+b)x^3a(ax2b)x+b^2$ and it provides curve points for the input values.
  - *Step* 8: Random point (k, m) is taken as public keys from the generated curve points.
- *Phase* 3: Signing Process
  - *Step* 9: Read first two bits of 128 bits from hashed message and consider as H(m).
  - *Step* 10: Find the S value by using the formula
$$S = (h^2 - H(M) * h) mod\ p$$
  - *Step* 11: Find the T value by using the formula
$$T = (h^2 - k * m) mod\ p$$
  - *Step* 12: Find the R value by using the formula
$$R = \left(\frac{S}{T}\right) mod\ p$$
  - *Step* 13: the R value is compressed by applying the formula C mod p=D. Here, each 8 bits of R value is considered as C and applied in the above formula.
  - *Step* 14: Compressed message digest value D is achieved.
  - *Step* 15: The D value is converted into signature using the newly created signature reference table is shown in Table 1.
  - *Step* 16: Produce the signature D
  - *Step* 17: Likewise, all 128 bits message digest H(M) are used and complete signature D is formed
- *Phase* 4: Verification Process
  - *Step* 18: Read the decrypted document that has been extracted from the cloud database.
  - *Step* 19: Apply SHA-512 hashing function to get H(M) value which is the 128 bits message digest.
  - *Step* 20: Initially 2 bits of 128 bits message digest will be taken as the H(M) value and processed to get the result for signature verification
  - *Step* 21: Find the U value of the document by applying the formula $U = (H(M) * h - k * m)\ mod\ p$
  - *Step* 22: Find the V by applying the formula
$$V = \left(1 - \left(\frac{U}{T}\right)\right) mod\ p$$
  - *Step* 23: The V value is compressed by applying the formula$C\ mod\ p = E$. Here, each 8 bits of V value is considered as C and applied in the above formula.
  - *Step* 24: Compressed message digest value E is achieved.
  - *Step* 25: The E value is converted into signature using the newly created signature reference table is shown in Table 1.

- *Step* 26: Produce the signature E.
- *Step* 27: Likewise, all 128 bits message digest are used and complete signature E is formed.

- *Phase* 5: Numerical to digital signature conversion Process
  - *Step* 28: Read the 64 bits signature generated by the signing process as well as the verification process.
  - *Step* 29: Compare each single bit number present in the numerical signature with the Signature reference table (Table 1).
  - *Step* 30: Every single numerical signature value has three key values of different forms.
  - *Step* 31: When the number appears first time in the signature first row key value is taken for signature.
  - *Step* 32: When the same number appears second time in the signature, then the second-row value is taken as a key.
  - *Step* 33: When the same number repeats third time also, the third-row key value is taken.
  - *Step* 34: Again, if the number keeps on repeating again and again, the key assigning will be done again by the first row and next second row and so on. It will follow the circular process.
  - *Step* 35: After, getting the values of all numbers, stop the process and produce the completed signature for the comparison.

- *Phase* 6: Comparison Process
  - *Step* 36: Compare the signature D and E i.e., (D, E)
  - *Step* 37: If the signature D is equal to signature E then
    The document is "*genuine*".
    Else
    The document is "*fake*" or "*Modified*".
  - *Step* 38: Report the status of the document to the user through admin.

4.9. Numerical of Message Digest to Signature Reference Table

Table 1 consists of three stages as first time, second time and third time. These all the three stages are containing the characters, numerical values and symbols. Here, the specific number will occur the first time then it takes the key values from the first stage of the signature reference table. Second, the same number will occur second time, then it will replace with the key values that are available in second time in the respective numerical value or number. Third, if the same number will occur third time than it takes the key values that are available in the third stage of the signature reference table. In case, the specific number will repeat more than three times then the first stage is considered as fourth and so on. The next occurring value will be considered the key values of the next stages. By comparing the message digest with the signature reference table, the final digital signature is produced

Table 1. Numerical of message digest to signature reference table.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1st Time	Z	Y	X	W	V	U	T	S	R	Q
2nd Time	9	8	7	6	5	4	3	2	1	0
3rd Time	!	@	#	$	%	&	*	+	-	/

- **Digital signature (64 bits)**: this is the sample64-bit digital signature which is produced by the proposed EDSA algorithm that comprises of symbols, numbers and characters for improving complexity level.

YTZR9S8!@XY38!@XY387@*YZ929!YWZ19#!T8
VZ+9Q!3Z-@59UY!ZR86@9Y%8!Z94!$

5. Results and Discussion

This section describes in detail about the experimental setup and the various experiments have been conducted for demonstrating the performance of the proposed EDSA. These all experimental results proved that the efficiency of EDSA by performing the comparative analysis.

5.1. Experimental Setup

The experiments have been conducted for measuring the performance of the newly proposed Enhanced Digital Signature Algorithm which is developed for generating a digital signature for providing the integrity of stored documents in cloud database. Here, we have used J2EE7, the software Java System Development Kit (JSDK) 8.1 version, Windows 10, private cloud called DriveHQ. Moreover, we have used MySQL8.0 as a database for storing the data. In addition, the standard application Server called Apache Tomcat 8.0.27 is also used for conducting the experiments.

5.2. Experimental Results and Discussion

Figure 6 shows the signing time analysis for the proposed digital signature approach called EDSA and the standard digital signature algorithms including RSA and ECDSA. Here, the different bit sizes were considered in the proposed digital signature scheme and the existing schemes. Generally, 1024 bit of RSA key length is equivalent to 192 bits of ECDSA key length. For this reason, we have considered the RSA key length from 512 bits and ECDSA from 64 bits.

From Figure 6, it can be seen that the signing time of the proposed EDSA is less while comparing with other digital signature schemes such as RSA and ECDSA. Here, the reason for consuming less time is to perform signing process due to the use of new formulas.

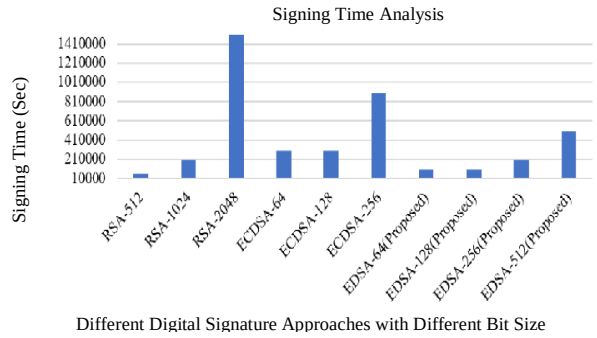

Figure 6. Signing time analysis.

Figure 7 is demonstrated that the verification time analysis between the proposed digital signature algorithm and standard digital signature schemes such as RSA and ECDSA. Moreover, the different bit sizes were considered in all these digital signature schemes.

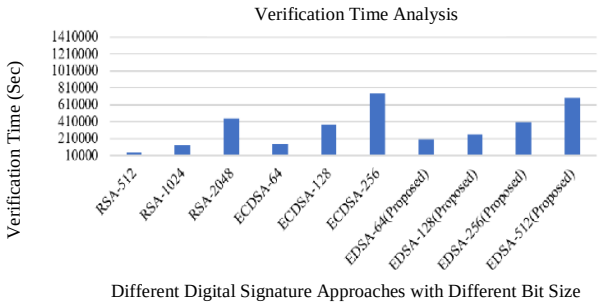

Figure 7. Verification time analysis.

From Figure 7, it can be observed that the verification time of the proposed digital signature algorithm is less in all bit sizes than the standard and available digital signature methods like RSA and ECDSA in various bit sizes. The introduction of new verification formulas is the reason for better performance than other digital signature approaches.

Figure 8 shows the key generation time analysis between the proposed digital signature scheme and the existing digital signature schemes like RSA and ECDSA. Here, the time analysis has been done by considering the various bit sizes in the proposed and existing digital signature schemes.

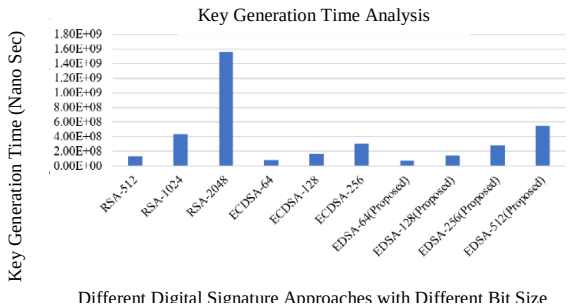

Figure 8. Key Generation Time Analysis.

The proposed digital signature scheme consumed less time for generating keys when compared with other existing digital signature schemes due to the use of elliptic curve square point as public keys. Moreover, we have also incorporated the existing SHA-512 algorithm for producing H(M) value in the proposed digital signature scheme.

Generally, the security level of RSA, ECDSA and the proposed EDSA are high, the complexity of RSA is built according to the Integer factorization and the complexity of ECDSA and the proposed EDSA are based on discrete logarithm. Table 2 shows the performance level comparison of key generation, processing, verification and signing that are represented as Higher, High and Low. From Table 3, it can be seen that the hashed message of the proposed work contains numeric, non-numeric and symbols which is different from other hashed messages of various existing hashing techniques. The bit size is minimum than few existing hashing techniques. Here, the usage of symbols provides more complexity to the attackers for predicting the hashing technique.

6. Conclusions and Future Work

An EDSA has been proposed and implemented in this work to perform secured data storage in cloud and it also used for accessing the cloud data. This proposed EDSA has been developed according to the Elliptic Curve Square points that are generated by using an upgraded equation. Moreover, these elliptic curve points were used as a public key which is used for performing the signing and verification processes. Moreover, a new base formula is also introduced for performing digital signature operations such as signing and verification. In addition, a new compression technique has been used for reducing the bit size of the signature. Here, the integrity and the originality of the data have been assured by output of the comparative analysis result of the signature and verification values. The experimental results proved that the efficiency of the proposed EDSA by conducting various experiments with less key generation time, signing time and verification time. Moreover, the compressed form of signature with 64 bits has been achieved that reduces the signature comparison time. Further works can be done in this direction by introducing new digital signature algorithms for enhancing the privacy preservation and efficiency.

References

[1] Bellare M. and Neven G., "Transitive Signatures: New Schemes and Proofs," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 2133-2151, 2005.

[2] Bjelland P., Franke K., and Arnes A., "Practical use of Approximate Hash Based Matching in Digital Investigations," *Digital Investigation*, vol. 11, no. 1, pp. 18-26, 2014.

[3] Blahut R., *Cryptography and Secure Communication*, Cambridge University Press,

2014.

[4] Chang C. and Chang Y., "Signing A Digital Signature Without Using One-Way Hash Functions and Message Redundancy Schemes," *IEEE Communications Letters*, vol. 8, no. 8, pp. 485-487, 2004.

[5] Chen X., Zhang F., Susilo W., Tian H., Li J., and Kim K., "Identity-Based Chameleon Hashing and Signatures without Key Exposure," *Information Sciences*, vol. 265, pp. 198-210, 2014.

[6] Gao W., Li F., and Wang X., "Chameleon Hash without Key Exposure Based on Schnorr Signature," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 282-285, 2009.

[7] Huang Q., Ma Z., Yang Y., Xinxin N., and Jingyi F., "Attribute Based DRM Scheme with Dynamic Usage Control in Cloud Computing," *China Communications*, vol. 11, no. 4, pp. 50-63, 2014.

[8] Huang X. and Wang W., "A Novel and Efficient Design for an RSA Cryptosystem with a Very Large Key Size," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 62, no. 10, pp. 972-976, 2015.

[9] Ismail E., Tahat N., and Ahmad R., "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms," *Journal of Mathematics and Statistics*, vol. 4, no. 4, pp. 222-225, 2008.

[10] Jaidi F., Ayachi F., and Bouhoula A., "Advanced Analysis of the Integrity of Access Control Policies: the Specific Case of Databases," *The International Arab Journal of Information Technology*, vol. 17, no. 5, pp. 808-815, 2020.

[11] Jiang L. and Guo D., "Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage," *IEEE Access*, vol. 5, pp. 13336-13345, 2017.

[12] Kaaniche N. and Laurent M., "Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms," *Computer Communications*, vol. 111, pp 120-141, 2017.

[13] Kavin B. and Ganapathy S., "A Secured Storage and Privacy-Preserving Model Using CRT for Providing Security on Cloud and Iot-Based Applications," *Computer Networks*, vol. 151, pp. 181-190, 2019.

[14] Kim J. and Oh H., "FAS: Forward Secure Sequential Aggregate Signatures for Secure Logging," *Information Sciences*, vol. 471, pp. 115-131, 2019.

[15] Kumar S., Kumar M., Budhiraja R., Das M., and Singh S., "A Cryptographic Model for Better Information Security," *Journal of Information Security and Applications*, vol. 43, pp. 123-138, 2018.

[16] Kumar M. and Srivastava S., "Image Authentication by assessing Manipulations using Illumination," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 12451-12463, 2018.

[17] Kumar M., Srivastava S., and Uddin N., "Forgery Detection Using Multiple Light Sources for Synthetic Images," *Australian Journal of Forensic Sciences*, vol. 51, no. 3, pp. 243-250, 2017.

[18] Li T., Liu Z., Li J., Jia C., and Li K., "CDPS: A Cryptographic Data Publishing System," *Journal of Computer and System Sciences*, vol. 89, pp 80-91, 2017.

[19] Liu X., Zhang Y., Wang B., and Yan J., "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1182-1191, 2013.

[20] Lou D. and Liu J., "Fault Resilient and Compression Tolerant Digital Signature for Image Authentication," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 31-39, 2000.

[21] Mitchell C., "On the Security of 2-Key Triple DES," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6260-6267, 2016.

[22] Muthurajkumar S., Vijayalakshmi M., Kannan A., and Ganapathy S., "Optimal and Energy Efficient Scheduling Techniques for Resource Management in Public Cloud Networks," *National Academy Science Letters*, vol. 41, no. 4, pp. 219-223, 2018.

[23] Perbawa M., Afryansyah D., and Sari R., "Comparison of ECDSA and RSA Signature Scheme on NLSR Performance," *in Proceedings of IEEE Asia Pacific Conference on Wireless and Mobile*, Bandung, pp. 7-11, 2017.

[24] Rani A. and Kumar., "Review on Cryptographic WLAN Protocols and Their Weakness," *International Journal of Emerging Trends in Engineering and Development*, vol. 2, no. 3, pp. 343-354, 2013.

[25] Rivest R., Shamir A., and Adleman L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[26] Selim A, "Digital Signatures: A Tutorial Survey," *Computer-IEEE Computer Society*, vol. 16, pp. 15-24, 1983.

[27] Sohal M. and Sharma S., "BDNA-A DNA Inspired Symmetric Key Cryptographic Technique to Secure Cloud Computing," *Journal of King Saud University-Computer and Information Sciences*, 2018.

[28] Stallings W., *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 2011.

[29] Tysowski P. and Hasan M., "Hybrid Attribute- and Re-Encryption based Key Management for

Secure and Scalable Mobile Applications in Clouds," *IEEE Transactions on Cloud Computing*, vol. 1, no. 2, pp. 172-186, 2013.

[30] Wang Y., Ni L., Chang C., and Yu H., "DW-AES: A Domain-Wall Nanowire-Based AES for High Throughput and Energy-Efficient Data Encryption in Non-Volatile Memory," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2426-2440, 2016.

[31] Xue Y., Tan Y., Liang C., Li Y., Zheng J., and Zhang Q., "Root Agency: A Digital Signature-Based Root Privilege Management Agency For Cloud Terminal Devices," *Information Sciences*, vol. 444, pp. 36-50, 2018.

[32] Yen S. and Laih C., "Fast Algorithms for LUC Digital Signature Computation," *IEE Proceedings-Computers and Digital Techniques*, vol. 142, no. 2, pp. 165-169, 1995.

[33] Yu J., Lu P., Zhu Y., Xue G., and Li M., "Toward Secure Multi keyword Top-k Retrieval over Encrypted Cloud Data," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 239-250, 2013.

[34] Zhang C., "Integrated Approach for Fault Tolerance and Digital Signature in RSA," *IEEE Proceedings-Computers and Digital Techniques*, vol. 146, no. 3, pp. 151-159, 1999.

[35] Zhang J. and Wang Y., "An Improved Signature Scheme without Using One-Way Hash Functions," *Applied Mathematics and Computation*, vol. 170, no. 2, pp. 905-908, 2005.

[36] Zhou L., Varadharajan V., and Hitchens M., "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1947-1960, 2013.

Balasubramanian Prabhu Kavin is currently working as a Lecturer in Sri Ramachandra Institute of Higher Education and Research, Sri Ramachandra Faculty of Engineering and Technology, Chennai. He received his Ph.D in Computer Science and Engineering from VIT-Chennai Campus, Chennai in the area of Cloud Computing and Security. He has completed his M.E. from Anna University, Chennai. He has published 7 papers in journal and conference. His areas of interest are Cryptography, Cloud Computing and Security.

Sannasi Ganapathy is currently working as Assistant Professor (Sr. Gr) in VIT University, Chennai. He received his M.E and Ph. D degrees from Anna University, Chennai. He has published more than 80 articles in journals and conferences. His area of interest includes Computer Networks, Soft Computing, Cloud Computing and Security.